UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/830,180	04/23/2001	George Bilchev	36-1442	2964

23117 7590 06/22/2005

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/830,180	**Applicant(s)** BILCHEV, GEORGE	
	Examiner Ponnoreay Pich	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _21 April 2005_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-83_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-83_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-83 have been examined and are pending. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Amendment

The examiner has noted applicant's amendments to the specification and abstract filed 4/21/2005.

Response to Arguments

Applicant's arguments filed 4/21/2005 have been fully considered but they are not persuasive.

Applicant first states that claim 1 requires functional modules sequentially coupled to operate on data blocks and that each functional module is claimed so as to include a data processing unit having parallel input and parallel output and to perform a reversible process on bits applied to the input and a configuring means which selects a set of the bits of a data processing unit to produce at the data processing output, a replacement set of bits for the originally selected bits. Applicant then discussed a preferred embodiment of applicant's invention as disclosed in the specification and states that Wilson operates on a different principle. Applicant does not believe the matrix 10 and XOR gates 30 disclosed by Wilson constitute a functional module of applicant's invention. Applicant does not believe the modules are sequentially coupled functional modules. Nor does applicant believe there is any sense in which there is a selection of a set of the input bits to apply to a data processing unit.

The examiner disagrees with the above analysis of Wilson by applicant. If one were to look at Figure 1 disclosed by Wilson, the examiner believes that each of the boxes or group of boxes shown reads on functional modules. More particularly, the examiner believes that the Shift Register 18 along with the AND gates it is connected with constitutes one functional module having parallel input and parallel output. Note that the input into the Shift register consist of the Buffer Memory data and a clock signal. There may also be an enable signal line not shown depending on the exact type of shift register used. These lines together reads on parallel inputs. The outputs from the AND gates reads on parallel outputs. The Central Memory unit 10 also reads on another functional module. It is connected in sequence with the functional module consisting of the Shift Register 18 and the group of AND gates CA(sub(0))-CA(sub(63)). Functional module 10 also obviously has parallel inputs and outputs. The next functional module consists of the Shift Register 32 and the XOR gates 30 it is connected to. Obviously all three functional modules are connected to each other in sequence. As to applicant's argument that the units disclosed by Wilson does not read on applicant's preferred embodiment as disclosed in the specification, applicant is reminded that the rejection only has to meet the claim language, not limits from the specification. As to applicant's argument of there not being any sense in which there is a selection of a set of the input bits to apply to a data processing unit, applicant is directed towards the first functional module discussed above which consists of Shift Register 18 and the group of AND gates. Obviously the data from buffer memory 18 is most likely serial in nature coming into the register 18. However, by using the shift register to shift the bits of the data and the AND gates, the data is made parallel going into the next functional module. Obviously, the data going into each of the different input lines of module 10 are different. The AND operations done in the first functional unit constitutes the selection of a set of input bits. Obviously the output bits from the first functional unit are replacements of the input data bits going into the first functional unit, so there would be no need to "modify" Wilson as applicant suggests. When Wilson was used in rejections in combination with Feistel, obviously even though Feistel might not disclose the above limitations, Wilson did, so applicant's arguments that Feistel did not disclose the above limitations are moot.

Applicant then argues that one of ordinary skill would not to think that Wilson could be improved by adding the Feistel concept or that Feistel could be improved by adding the Wilson concept because their enciphering concepts are based on different principles. The examiner disagrees with this also. Note that Wilson discloses that his encryption concept is based on encryption as a set of blocks or block encryption systems (col 1, lines 6-11). Feistel discloses that his system is based on either a stream or block cipher mode (abstract, lines 1-3). Obviously since they both operate on block ciphering, they are related in principles.

Applicant then stated that with regard to claim 71, applicant does not believe Feistel discloses a random number generator of the claimed limitation. More particularly, applicant cannot identify where in the cited passages a pseudo-random number is encoded to provide respective descriptions of predetermined sets of bits of a data block as received at the respective module's input. The cited passages in question are column 3, lines 62-66, column 5, lines 6-20; and the abstract, last sentence. Examining the passages in question, it is clear from the last sentence of the abstract that there is a pseudo-random number generator: "...the second key is entered in its entirety into the system where it is successively and continuously transformed as a function of said first key whereby the function of said system becomes a **pseudo-random number generator**...." The transformation of the second key, which is obviously a pseudo-random number as most keys are, reads on the pseudo-random number being encoded. Column 3, lines 62-66 also mentions a "pseudo-random number generator" described in the abstract. As this number is used for encryption of data, it must provide respective descriptions of predetermined sets of bits of a data block as received at the respective module's input.

The applicant also does not believe there is a cascade of modules where the output of one module is coupled to the input of the following module. Note Figure 1. Each of the boxes represents modules. Obviously the output from one module is connected to the input of another module, so there is cascading of modules. Consider also column 5, lines 6-20, which was cited. The transformation of the data are functions of the keys, therefore the keys provide a description of respective predetermined sets of bits as received at a module input.

The examiner believes that he has addressed all of the applicant's arguments filed on 4/21/2005 and have shown that applicant's claims as recited are not in a condition of allowance. Any rejections not argued, the examiner assumes applicant agrees with. The examiner has copied and pasted the previous examiner's rejection from the previous non-final action below so that it may be easily referenced.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 10-26, 30-41, 43-61, 65-70, 79-83 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wilson (4520232).

With respect to Claim 1, the limitation of "forming means for receiving the signal to be enciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits" is met on column 2, lines 44-46, 58-62; and "a plurality of encipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means" on column 2, lines 19-31; and "configuring means, wherein each encipher functional module comprises a module input, a module output" is met on Fig. 1; and "a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits" is met on Fig. 1 and on column 1, lines 36-39, 64-68; and "is operable under the control of the configuring means to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output an enciphered data block in which said respective predetermined set of bits is replaced by the corresponding enciphered set of bits produced at the parallel output of its data processing unit" is met on column 2, lines 19-23, 44-49; column 3, lines 10-56. Wilson however does not explicitly show a configuring means.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have a configuring means that coordinates the inputting, enciphering and outputting of information because the given steps are coordinated and effectively achieved in the reference. Hence the existence of a configuring means is obvious.

With respect to Claim 2, the limitation of "wherein said respective data processing units are of a single type" is met on Fig. 1. The shift register and corresponding set of gates occur multiple times.

With respect to Claim 3, the limitation of "wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the set of bits received at its parallel input" is met on column1, lines 35-60.

With respect to Claim 4, the limitation of "wherein each of said data processing units is a reversible gate" is met by Fig. 1. The AND gate(s) is reversible.

With respect to Claim 5, the limitation of "wherein said reversible gate comprises a Fredkin's gate or an AND/NAND gate" is met by Fig. 1.

With respect to Claim 6, the limitation of "wherein said configuring means is operative to control said encipher functional modules in accordance with a cipher design description" is met on column 4, lines 55-63; column 1, lines 29-33.

With respect to Claim 7, the limitation of "including means for receiving said cipher design description" is met on column 3, lines 66-68; column 4, lines 1-14.

With respect to Claim 8, the limitation of "including means for generating said cipher design description" is met on column 4, lines 55-63.

With respect to Claim 10, the limitation of "wherein each said encipher functional module comprises a logic gate which does not conserve logic" is met by Fig. 1.

With respect to Claim 11, the limitation of "wherein said plurality of encipher functional modules form a programmable circuit" is met by the abstract and by Fig. 1.

With respect to Claim 12, the limitation of "wherein said plurality of encipher functional modules comprises a programmable logic gate array, and said configuring means comprises a programming means for programming said programmable logic gate array" is met by Fig. 1 and the abstract.

With respect to Claim 13, the limitation of "wherein said encipher functional modules comprise analogue electronic modules" is met on column 2, lines 58-62.

With respect to Claim 14, the limitation of "wherein said signal is an optical signal and said encipher functional modules comprise optical components" is met on column 4, lines 49-51. It would have been obvious to one of ordinary skill in the art at the time of the invention to have the existence of the modem within the network make the existence of optical components obvious because a modem implies that some form of transmitted signals are sent between two remote terminals and processed.

With respect to Claim 15, the limitation of "a programmable computing apparatus, wherein said encipher functional modules comprise a computer code routine implemented on said programmable computing apparatus" is met by Fig. 1 and the abstract.

With respect to Claim 16, the limitation of "wherein said computer code routine is in the form of a generic module code routine repeatedly implemented dependent upon information from said configuring means" is met on column 4, lines 55-68.

With respect to Claim 17, the limitation of "including first selection means for selecting a type of encipher functional module to be used from amongst a plurality of possible types of encipher functional modules, wherein said configuring means is adapted to configure the encipher apparatus to use the selected type of encipher functional module" is met on column 3, lines 23-37.

With respect to Claim 18, the limitation of "including second selection means for selecting the number of said encipher functional modules to be used, wherein said configuring means is adapted to configure the encipher apparatus to use the selected number of encipher functional modules" is met on column 3, lines 23-37.

With respect to Claim 19, the limitation of "third selection means for selecting for each said encipher functional module the respective predetermined set of the bits of a data block received at its module input" is met on column 3, lines 23-37.

With respect to Claim 20, the limitation of "receiving the signal to be enciphered and forming the signal into a sequence of data blocks, each having a first predetermined number of bits" is met on column 2, lines 44-46, 58-62; and "applying the sequence of data blocks to a plurality of encipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks" is met on column 2, lines 19-31; and "each encipher functional module comprising a module input, a module output, and a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits" is met by Fig. 1 and on column 1, lines 36-39, 64-68; and "configuring each encipher functional module to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output an enciphered data block in which said respective predetermined set of bits is replaced by the corresponding enciphered set of bits produced at the parallel output of its data processing unit" is met on column 2, lines 19-23, 44-49 and on column 3, lines 10-56. Wilson et al however does not explicitly show configuration of the cipher functional modules.

It would have been obvious to one of ordinary skill in the art at the time of the invention to configure the cipher modules so as to enable the inputting, enciphering and outputting of information because the given steps are coordinated and effectively achieved in the reference. Hence configuring the cipher functional modules to achieve this is obvious.

With respect to Claim 21, the limitation of "wherein the encipher functional modules are of a single type" is met by Fig. 1.

With respect to Claim 22, the limitation of "wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input" is met on column 1, lines 35-60.

With respect to Claim 23, the limitation of "wherein said encipher functional modules each act as a reversible gate" is met by Fig. 1.

With respect to Claim 24, the limitation of "wherein the configuring of said encipher functional modules is in accordance with a cipher design description" is met on column 4, lines 55-63 and on column 1, lines 29-33.

With respect to Claim 25, the limitation of "including receiving said cipher design description" is met on column 3, lines 66-68 and on column 4, lines 1-14.

With respect to Claim 26, the limitation of "including generating said cipher design description" is met on column 4, lines 55-63.

With respect to Claim 30, the limitation of "wherein said encipher functional modules comprise a programmable logic gate array and the configuring step includes programming said programmable logic gate array" is met by the abstract and on Fig. 1.

With respect to Claim 31, the limitation of "implemented by computer code on a computing apparatus, wherein said encipher functional modules comprise a computer code routine implemented in dependence upon configuration information" is met on column 4, lines 55-68.

With respect to Claim 32, the limitation of "wherein the computer code routine is implemented repeatedly dependent upon the number of said encipher functional modules to be implemented" is met on column 4, lines 55-68.

With respect to Claim 33, the limitation of "including selecting the type of encipher functional module to be used from amongst a plurality of possible types of encipher functional modules" is met on column 3, lines 23-37.

With respect to Claim 34, the limitation of "including selecting the number of said encipher functional modules used" is met on column 3, lines 23-37.

With respect to Claim 35, the limitation of "including selecting the respective predetermined set of the bits of a received data block for said encipher functional modules" is met on column 3, lines 23-37.

With respect to Claim 36, the limitation of "forming means for receiving the signal to be deciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits" is met on column 1, lines 64-68 and on column 2, lines 58-62; and "a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means" is met on column 2, lines 19-31; and "configuring means, wherein each decipher functional module comprises a module input and a module output" is met by Fig. 1 and "a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits" is met by Fig. 1 and on column 1, lines 36-39, 64-68; and "is operable under the control of the configuring means to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit" is met on column 2, lines 19-23; column 4, lines 55-64; and column 5, lines 1-17. Wilson however does not explicitly describe a configuring means.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have a configuring means that coordinates the inputting, enciphering and outputting of information because the given steps are coordinated and effectively achieved in the reference. Hence the existence of a configuring means is obvious.

With respect to Claim 37, the limitation of "wherein said decipher functional modules are of a single type" is met by Fig. 1.

With respect to Claim 38, the limitation of "wherein said configuring means is operative to control said decipher functional modules in accordance with a cipher design description" is met on column 1, lines 29-33; column 4, lines 55-64.

With respect to Claim 39, the limitation of "wherein said cipher design description is equivalent to the inverse of a cipher design description used to control encipher functional modules of an encipher apparatus used to produce the enciphered signal" is met on column 5, lines 1-6.

With respect to Claim 40, the limitation of "including means for receiving said cipher design description" is met on column 4, lines 55-64.

With respect to Claim 41, the limitation of “including means for generating said cipher design description” is met on column 4, lines 55-64.

With respect to Claim 43, the limitation of “wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input” is met on column 1, lines 35-60.

With respect to Claim 44, the limitation of “wherein each of said data processing units comprises a reversible gate” is met by Fig. 1.

With respect to Claim 45, the limitation of “wherein said reversible gate comprises a Fredkin's gate or an AND/NAND gate” is met by Fig. 1.

With respect to Claim 46, the limitation of “wherein each said decipher functional module comprises a logic gate which does not conserve logic” is met by Fig. 1.

With respect to Claim 47, the limitation of “wherein said plurality of decipher functional modules form a programmable circuit” is met by the abstract and by Fig. 1.

With respect to Claim 48, the limitation of “wherein said plurality of decipher functional modules comprise a programmable logic gate array, and said configuring means comprises a programming means for programming said programmable logic gate array" is met by the abstract and by Fig. 1.

With respect to Claim 49, the limitation of "wherein said signal is an optical signal and said decipher functional modules comprise optical components" is met on column 4, lines 49-51.

With respect to Claim 50, the limitation of "wherein said decipher functional modules comprise a computer code routine implemented on said programmable computing apparatus" is met by Fig. 1 and in the abstract.

With respect to Claim 51, the limitation of "wherein said decipher functional modules comprise a computer code routine repeatedly implemented dependent upon information from said configuring means" is met on column 4, lines 55-68.

With respect to Claim 52, the limitation of "wherein said configuring means is responsive to type identifying information included in a cipher design description to configure the type of said decipher functional modules in accordance with said type identifying information" is met on column 2, lines 49-53.

With respect to Claim 53, the limitation of "wherein said configuring means is responsive to module number information included in a cipher design description to configure a corresponding number of said decipher functional modules" is met on column 4, lines 55-62.

With respect to Claim 54, the limitation of "wherein said configuring means is responsive to data block size information included in a cipher design description adapted to configure the input and output of each said decipher functional module" is met on column 4, lines 55-64.

With respect to Claim 55, the limitation of "receiving the signal to be deciphered and outputting the signal as a sequence of data blocks, each having a first predetermined number of bits" is met on column 1, lines 64-68; column 2, lines 58-62; and "applying the sequence of data blocks to a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks" is met on column 2, lines 19-31; and "each decipher functional module comprising a module input, a module output" is met by Fig. 1; and "a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits" is met by Fig. 1 and on column 1, lines 36-39, 64-68; and "configuring each decipher functional module to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output an deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit" is met on column 2, lines 19-23; column 4, lines 55-64; and column 5, lines 1-17. Wilson et al however does not explicitly show configuration of the decipher functional modules.

It would have been obvious to one of ordinary skill in the art at the time of the invention to configure the decipher modules so as to enable the deciphering and outputting of the given deciphered information because the given steps are coordinated and effectively achieved in the reference. Hence configuring the decipher functional modules to achieve this is obvious.

With respect to Claim 56, the limitation of "wherein the decipher functional modules are of a single type" is met by Fig. 1.

With respect to Claim 57, the limitation of "wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input" is met on column 1, lines 35-60.

With respect to Claim 58, the limitation of "wherein said decipher functional modules each act as a reversible gate" is met on column 1, lines 36-41, 64-68.

With respect to Claim 59, the limitation of "wherein the configuring of said decipher functional modules is in accordance with a cipher design description" is met on column 1, lines 29-33; column 4, lines 55-64.

With respect to Claim 60, the limitation of "including receiving said cipher design description" is met on column 4, lines 55-64.

With respect to Claim 61, the limitation of "including generating said cipher design description" is met on column 4, lines 55-64.

With respect to Claim 65, the limitation of "wherein said decipher functional modules comprise a programmable logic gate array and the configuring step includes programming said programmable logic gate array" is met by the abstract and by Fig. 1.

With respect to Claim 66, the limitation of "implemented by computer code on a computing apparatus, wherein said decipher functional modules comprise a computer code routine implemented in dependence upon configuration information" is met on column 4, lines 55-68.

With respect to Claim 67, the limitation of "wherein the computer code routine is implemented repeatedly dependent upon the number of said decipher functional modules to be implemented" is met on column 5, lines 1-17.

With respect to Claim 68, the limitation of “including selecting the type of decipher functional module to be used from amongst a plurality of possible types of decipher functional modules” is met on column 3, lines 23-37.

With respect to Claim 69, the limitation of “including selecting the number of said decipher functional modules used” is met on column 3, lines 23-37.

With respect to Claim 70, the limitation of “including selecting the respective predetermined set of the bits of a received data block for said decipher functional modules” is met on column 2, lines 24-31.

With respect to Claim 79, its limitation is similar to Claim 36 limitation and hence its rejection can be found therein.

With respect to Claim 80, its limitation is similar to Claim 55 limitation and hence its rejection can be found therein.

With respect to Claim 81, its limitation is similar to Claim 20 limitation and hence its rejection can be found therein.

With respect to Claims 82 and 83, its rejection can be found within Claim 20 rejection. The existence of a storage/carrier medium that stores the functions disclosed in Claim 20 is obvious.

Claims 9, 27-29, 42, 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wilson (4520232) in view of Feistel (4316055).

With respect to Claim 9, all the limitation is met by Wilson except for the following limitation.

The limitation of "wherein the generating means includes a random or pseudo-random number generator and is operative to use random or pseudo-random numbers generated by said random or pseudo-random number generator to describe in code said respective predetermined sets of bits" is met by Feistel in the abstract.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Feistel within the system of Wilson because a random output creates a more secure cipher. This is because a random number, when used as a seed to encrypt a cleartext, creates a more unique, harder-to-decrypt ciphertext.

With respect to Claim 27 and 62, all the limitation is met by Wilson except for the following limitation.

The limitation of “including generating random or pseudo-random numbers and using the generated random or pseudo-random numbers to generate said cipher design description” is met by Feistel in the abstract and on column 3, lines 50-54, 62-66.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Feistel within the system of Wilson because a random output creates a more secure cipher. This is because a random number, when used as a seed to encrypt a cleartext, creates a more unique, harder-to-decrypt ciphertext.

With respect to Claim 28, all the limitation is met by Wilson except for the following limitation.

The limitation of “wherein a respective generated random or pseudo-random number is used to described in code the respective predetermined set of bits for a respective said encipher functional module” is met by Feistel in the abstract.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Feistel within the system of Wilson because a random output creates a more secure cipher. This is because a random number, when used as a seed to encrypt a cleartext, creates a more unique, harder-to-decrypt ciphertext.

With respect to Claim 29, the limitation of “wherein the logic operations do not conserve logic” is met by Wilson on Fig. 1.

With respect to Claim 42, its limitation is similar to Claim 9 and hence its rejection can be found therein.

With respect to Claim 63, all the limitation is met by Wilson except for the following limitation.

The limitation of "wherein a respective generated random or pseudo-random number is used to described in code the respective predetermined set of bits for a respective said decipher functional module" is met on column 3, lines 50-54, 62-66.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Feistel within the system of Wilson because a random output creates a more secure cipher. This is because a random number, when used as a seed to encrypt a cleartext, creates a more unique, harder-to-decrypt ciphertext.

With respect to Claim 64, the limitation of "wherein the logic operations do not conserve logic" is met by Wilson on Fig. 1.

Claims 71-78 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel (4316055).

With respect to Claim 71, the limitation of "a random or pseudo-random number generator" is met on column 3, lines 62-66; and "encoding means arranged to receive a random or pseudo-random number generated by said generator and to encode that received number to provide at its output a cipher design description" is met in the abstract, last sentence; and "describing for each of a plurality of cipher functional modules sequentially coupled to operate sequentially on a data block applied to the plurality of sequentially coupled cipher functional modules, a respective predetermined set of the bits of the data block as received at the respective module's input" is met on column 5, lines 6-20.

With respect to Claim 72, the limitation of "including first selection means for selecting at least one type of cipher functional module to be used from amongst a plurality of possible types of cipher functional modules, said encoding means being adapted to include the selected type or types in the encoded information" is met on column 6, lines 63-66.

With respect to Claim 73, the limitation of "including second selection means for selecting the number of said cipher functional modules to be used, said encoding means being adapted to include the selected number in the encoded information" is met on column 7, lines 14-21.

With respect to Claim 74, the limitation of "including third selection means for selecting the number of inputs and outputs of said cipher functional modules, said encoding means being adapted to include the selected number in the encoded information" is met on column 6, lines 63-68 and on column 7, line 1.

With respect to Claim 75, the limitation of "generating random or pseudo-random numbers" is met on column 3, lines 62-66; and "encoding information, including said random or pseudo-random numbers, describing, for each of a plurality of cipher functional modules sequentially coupled to operate sequentially on a data block applied to the plurality of sequentially coupled cipher functional modules, a respective predetermined set of the bits of the data block as received at the respective module's input" is met in the abstract, last sentence and on column 5, lines 6-16; and "outputting the cipher design description" on column 5, lines 16-21.

With respect to Claim 76, the limitation of "selecting at least one type of cipher functional module to be used from amongst a plurality of possible types of cipher functional modules, and including the selected type or types in the encoded information" is met on column 7, lines 14-21.

With respect to Claim 77, the limitation of "selecting the number of said cipher functional modules used, and including in the encoded information said selected number of said cipher functional modules used" is met on column 7, lines 14-21.

With respect to Claim 78, the limitation of "selecting the number of inputs and outputs of said cipher functional modules, and including in the encoded information the selected number of inputs and outputs of said cipher functional modules" is met on column 6, lines 63-68 and on column 7, line 1.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100